ARTICOLO QUINTO

« **Sulle equazioni algebriche risolubili per radicali quadratici e sulla costruibilità dei poligoni regolari** » di FEDERIGO ENRIQUES a Bologna.

La questione di decidere se un problema geometrico costruttivo sia risolubile elementarmente, cioè operando sui dati, colla riga e col compasso, viene ricondotta dalla geometria analitica ad una questione algebrica.

Del modo come tale riduzione si effettua e delle osservazioni ad essa inerenti, discorre il signor CASTELNUOVO nell'articolo 4°. A noi basta qui ricordare la conclusione fondamentale:

Sia proposto un problema geometrico determinato, ricondotto alla ricerca dei punti di un piano che hanno relazioni prestabilite con certi punti dati nel piano stesso; affinchè la costruzione dei punti cercati si possa effettuare operando sui dati (e, se si vuole, anche sopra punti, rette e circoli arbitrari) cogli istrumenti riga e compasso, è condizione necessaria e sufficiente che le coordinate cartesiane dei punti incogniti si possano ottenere effettuando sopra le coordinate dei dati operazioni razionali e successive estrazioni di radicali quadratici (in numero finito).

Designeremo brevemente col nome di « *espressioni* (irrazionali) *quadratiche* » le espressioni formate operando sopra quantità date con operazioni razionali ed estrazioni di radicali quadratici; perciò, potremo enunciare l'anzidetta condizione di risolubilità d'un problema dicendo che: le coordinate dei punti incogniti debbono essere delle espressioni quadratiche formate colle coordinate dei dati.

Dimostreremo tra poco che ogni espressione quadratica soddisfa ad un' equazione algebrica i cui coefficienti si espri-

mono razionalmente per le quantità date, cioè sono razionali nel dato campo di razionalità. Con ciò la questione di decidere se un problema proposto sia risolubile elementarmente, verrà ricondotta alle due questioni seguenti:

1° decidere se il problema stesso (posto previamente sotto la forma innanzi accennata) sia *algebrico*, cioè venga a dipendere da un'equazione algebrica a coefficienti razionali nel campo dato;

2° decidere se una data equazione algebrica sia risolubile con operazioni razionali ed estrazioni di radicali quadratici, in un dato campo di razionalità a cui appartengono i coefficienti dell'equazione.

Riguardo alla prima questione notiamo che la geometria analitica insegna a tradurre le relazioni geometriche in relazioni analitiche; se queste ultime si presentano sotto forma algebrica, la questione anzidetta è subito risoluta affermativamente. Essa si presenta invece molto più difficile quando si pervenga a relazioni analitiche che non si presentino sotto forma algebrica, giacchè si tratta allora di riconoscere se queste relazioni analitiche (per quanto riguarda la determinazione delle incognite in un caso determinato) possano essere rimpiazzate con relazioni algebriche; tale ricerca conduce invero ai più alti problemi dell'analisi (cfr. art. 8°).

Noi vogliamo qui occuparci della seconda questione, dando un teorema generale sul grado delle equazioni algebriche risolubili con radicali quadratici. La questione non viene così esaurita (e per esaurirla si richiedono maggiori sviluppi); ma il resultato ottenuto basta alle applicazioni nel campo della Geometria elementare, che abbiamo in vista.

Fra queste applicazioni compariscono prima di tutto quelle relative alla costruzione dei poligoni regolari, che in questo stesso scritto trattiamo, e quelle relative ai problemi della duplicazione del cubo e della trisezione dell'angolo trattate nell'art. 7°.

Gli antichi ci hanno tramandato le costruzioni elementari del poligono regolare di 2^n lati, del triangolo equilatero e del pentagono regolare, nonchè quelle dei poligoni regolari di $2^n \cdot 3$ lati, $2^n \cdot 5$ lati, $3 \cdot 5$ lati, $2^n \cdot 3 \cdot 5$ lati, che dalle precedenti dipendono.

Ora si potrebbero cercare p. es. le costruzioni elementari dell'ettagono o del nonagono regolare, e mal ci si renderebbe

ragione delle difficoltà a cui si andrebbe incontro, quando non venisse fatto di porre in dubbio la risolubilità di tali problemi. Si accumulerebbero quindi inutili sforzi, senza trarre neppure dall'insuccesso un insegnamento qualsiasi intorno alla natura delle questioni proposte.

Ma chi avesse acquistato la persuasione che si tratta di questioni irresolubili, come oserebbe tentare la prova pei casi successivi nei quali le difficoltà vanno apparentemente crescendo? Dopo avere constatato, o supposto, che non sono costruibili elementarmente i poligoni regolari di 7, 9, 11, 13, 14 lati, come potrebbe venir in mente di cercare la costruzione di quello di 17 lati? Eppure accade in fatto che la costruzione dell'ettadecagono è possibile, mentre sono impossibili (colla riga e col compasso) le costruzioni dei poligoni regolari di 7, 9, 11, 13, 14 lati.

Di ciò rende ragione la bellissima teoria di GAUSS delle equazioni binomie.

La costruzione del poligono regolare di n lati viene a dipendere dalla risoluzione dell'equazione binomia

$$z^n = 1,$$

la quale, tolta la radice $z = 1$, si riduce alla

$$z^{n-1} + z^{n-2} + \ldots + 1 = 0.$$

Perchè lo ngono sia elementarmente costruibile occorre che la precedente equazione sia risolubile per radicali quadratici (nel campo di razionalità assoluto [1]). Ora tale risolubilità dipende dalla forma del numero n; precisamente l'equazione è risolubile se n, decomposto in fattori primi, è della forma

$$n = 2^{\nu}\left(2^{2^{\nu_1}}+1\right)\left(2^{2^{\nu_2}}+1\right)\ldots\left(2^{2^{\nu_s}}+1\right)$$

ove ν_1 ν_s.... ν_3 sono tutti differenti fra loro.

In questa formula sono dunque racchiusi tutti i poligoni regolari costruibili elementarmente (1).

Diamo qualche notizia particolareggiata su tali poligoni nel § 9 di questo articolo; e terminiamo con un cenno relativo

(1) Relativamente agli istrumenti da adoperarsi per le costruzioni il signor HILBERT ha osservato che l'uso del compasso può qui essere rimpiazzato dall'uso del *trasportatore di segmenti* (Cfr. art. 4°).

al problema dell'ettagono. Rimandiamo all' art. 6° per le svariate costruzioni dell' ettadecagono, di cui qui ci limitiamo a rilevare la possibilità teorica come conseguenza del teorema generale accennato.

Citeremo infine i principali lavori, ove si trovano svolte le teorie che formano oggetto del presente scritto, di cui ci siamo valsi nella compilazione di esso:

1°. Intorno alle equazioni algebriche risolubili per radicali quadratici:

PETERSEN: « *Teoria delle equazioni algebriche* », trad. it. ROZZOLINO e SFORZA. Napoli, Pellerano, 1891-92. — F. KLEIN: « *Conferenze sopra alcune questioni di geometria elementare* », trad. it. GIUDICE. Torino, Rosenberg e Sellier, 1896. — CAPELLI: « *Lezioni di Algebra complementare* ». Pellerano, Napoli, 1895.

2°. Per la teoria delle equazioni binomie in relazione al problema dei poligoni regolari:

GAUSS: « *Disquisitiones arithmeticae* « sectio VII, Werke Bd I. (1801). — P. BACHMANN: « *Die Lehre von der Kreistheilung...* » Leipzig, Teubner, 1872. — F. KLEIN: *l. c.* — L. BIANCHI: « *Lezioni sulla teoria delle sostituzioni e delle equazioni algebriche secondo Galois* ». Pisa, Nistri, 1896.

I.

§ 1. **Riduzione delle espressioni irrazionali quadratiche a forma normale.** — Consideriamo un' espressione (*quadratica*) x, formata con operazioni razionali e successive estrazioni di radicali quadratici a partire da certe quantità date $1, \alpha, \beta, \ldots$. che definiscono il nostro campo di razionalità $[1, \alpha, \beta, \ldots]$. Nella indicata espressione si troveranno *termini* contenenti un differente numero di radici sovrapposte, mediante i quali l'espressione stessa è razionalmente composta; diremo d'*ordine* m un termine nel quale figurano sotto uno stesso segno radicale altri $m - 1$ radicali. Così p. es.

$$\sqrt{a+\sqrt{b}}, \quad \sqrt{\sqrt{a}+\sqrt{b}}, \quad \sqrt{\sqrt{a}+\sqrt{b+\sqrt{c}}},$$

dove a, b, c rappresentano espressioni razionali, sono termini rispett. degli ordini 2, 3, 4.

Un termine d'ordine m si può designare con $\sqrt{X}$, dove X è un'espressione quadratica formata con termini d'ordine minore od uguale ad $m-1$.

Nell'espressione x si possono trovare dei termini d'ordine m, che sieno razionalmente esprimibili per i rimanenti termini d'ordine m e per quelli d'ordine inferiore; allora, rimpiazzando quei termini colle loro espressioni indicate, si può ridurre il numero dei termini che figurano in x.

Immaginiamo di avere effettuato ripetutamente finchè è possibile, tutte le riduzioni a cui danno luogo i termini d'ordine m costituenti x, quindi tutte le riduzioni a cui danno luogo i termini d'ordine $m-1$, e così via: avremo allora un'espressione di x nella quale il numero dei termini non è ulteriormente riducibile, nessun termine essendo esprimibile razionalmente per i rimanenti termini dello stesso ordine inferiore. Consideriamo partitamente ogni termine $\sqrt{X}$ di x, ed effettuiamo analogamente la riduzione di X al minimo numero dei termini. Proseguiamo nello stesso modo per ogni espressione che comparisca sotto qualche radicale in un termine di X, e così via. Fatte tutte le riduzioni possibili perveniamo infine ad una espressione di x, nella quale tutti i *radicali* sono *indipendenti*, sicchè il loro numero non è ulteriormente riducibile nel modo detto innanzi.

Per meglio spiegare la cosa prendiamo ad es.

$$x = \sqrt{\sqrt{a} + \sqrt{b} + \sqrt{ab}} + \sqrt{c} + \sqrt{d} + \sqrt{\frac{c}{d}}.$$

Possiamo rimpiazzare sotto il primo radicale

$$\sqrt{ab} \text{ con } \sqrt{a}\sqrt{b},$$

e ancora possiamo sostituire l'ultimo termine

$$\sqrt{\frac{c}{d}} \text{ con } \frac{\sqrt{c}}{\sqrt{d}};$$

dopo effettuate queste riduzioni si ha l'espressione

$$x = \sqrt{\sqrt{a} + \sqrt{b} + \sqrt{a}\cdot\sqrt{b}} + \sqrt{c} + \sqrt{d} + \frac{\sqrt{c}}{\sqrt{d}}$$

nella quale tutti i radicali sono indipendenti.

Dopo aver ridotto l'espressione di x a contenere radicali consideriamo in essa un termine del massimo ordine m, sia $\sqrt{X}$; la x si può riguardare come un'espressione razionale di $\sqrt{X}$ i cui coefficienti $a_1 a_2 \ldots$, $b_1 b_2 \ldots$ sono formati razionalmente cogli altri termini; dunque

$$x = \frac{a_1 + a_2\sqrt{X} + a_3(\sqrt{X})^2 + \ldots + a_n(\sqrt{X})^n}{b_1 + b_2\sqrt{X} + b_3(\sqrt{X})^2 + \ldots + b_m(\sqrt{X})^m}.$$

Ma poichè

$$(\sqrt{X})^2 = X, \quad (\sqrt{X})^4 = X^2 \ldots,$$

si potrà porre

$$x = \frac{l + m\sqrt{X}}{r + s\sqrt{X}},$$

dove l, m, r, s dipendono razionalmente dai termini d'ordine m, diversi da $\sqrt{X}$, e da termini d'ordine inferiore. Ora

$$x = \frac{l + m\sqrt{X}}{r + s\sqrt{X}} = \frac{(l + m\sqrt{X})(r - s\sqrt{X})}{(r + s\sqrt{X})(r - s\sqrt{X})},$$

$$= \frac{lr - msX}{r^2 - s^2X} + \left(\frac{mr - ls}{r^2 - s^2X}\right)\sqrt{X},$$

ossia

$$x = A + B\sqrt{X},$$

ove A e B dipendono razionalmente dagli altri termini d'ordine m, $\sqrt{Y}$, $\sqrt{Z}\ldots$, e da termini d'ordine inferiore.

Prendiamo a considerare successivamente le espressioni A e B. Ciascuna di esse, p. es. A, può essere posta relativamente a $\sqrt{Y}$ sotto una forma analoga a quella ottenuta per x:

$$A = A_1 + A_2\sqrt{Y},$$

dove A_1 e A_2 sono composti razionalmente con $\sqrt{Z}\ldots$, e con termini d'ordine minore di m.

Operando nello stesso modo sopra le nuove espressioni A_1, A_2 ecc. perveniamo infine a rappresentare la x con un'espressione intera dei termini d'ordine m

$$\sqrt{X}, \quad \sqrt{Y}, \quad \sqrt{Z}\ldots,$$

dove questi termini compariscono soltanto moltiplicati fra loro, ma non elevati a potenza; i coefficienti d'una tale espressione dipenderanno razionalmente da termini d'ordine minore di m.

È chiaro che la riduzione di forma operata relativamente ai termini d'ordine m, si può effettuare successivamente in relazione ai termini d'ordine $m-1$, che entrano in x o nelle espressioni X, Y, Z...., poi in relazione ai termini d'ordine $m-2$ e così via. Giungeremo infine ad un'espressione di x che chiameremo *forma normale*, la quale sarà costruita (a partire da quantità razionali sul campo dato) con sole operazioni di addizione, di moltiplicazione e di estrazione di radice quadrata, ciascun radicale quadratico figurando soltanto alla prima potenza.

I ragionamenti successivi che istituiremo sulle espressioni quadratiche si basano sull'ipotesi che esse sieno preliminarmente ricondotte a contenere *radicali indipendenti sotto forma normale;* il numero di questi radicali può allora designarsi col nome di *grado* dell'espressione quadratica.

§ 2. **Formazione di un'equazione algebrica a cui soddisfa un'espressione quadratica.** — *Un' espressione quadratica* x, *di grado* n, *soddisfa ad un' equazione algebrica di grado* 2^n, *a coefficienti razionali* (nel dato campo di razionalità).

Immaginiamo di dare agli n radicali che entrano nell'espressione x tutti i valori (positivi e negativi) che essi possono ricevere; otteniamo così 2^n valori di x: x_1, x_2, ... x_i .... x_{2^n}, alcuni dei quali (come mostreremo fra poco) potranno essere uguali fra loro.

Costruiamo l'equazione

$$f(x)=(x-x_1)(x-x_2)....(x-x_{2^n})=x^{2^n}+p_1x^{2^n-1}+....+p_{2^n}=0$$

che ha per radici le x_i.

I coefficienti di tale equazione si esprimono colle funzioni simmetriche elementari delle x_i, per mezzo delle formule

$$p_1=-\Sigma x_i$$
$$p_2=\Sigma x_i x_k$$
$$\cdots\cdots\cdots$$
$$p_{2^n}=x_1x_2....x_n.$$

Si tratta di provare che questi coefficienti sono razionali.

Questa proprietà risulta dal fatto fondamentale che le p_r sono funzioni *simmetriche* delle x_i, cioè che esse rimangono inalterate quando si permuti in un modo qualsiasi l'ordine delle x_i (p. es.

$$p_1 = -(x_1 + x_2 + \ldots + x_{2^n}) = -(x_2 + x_1 + x_3 + \ldots + x_{2^n}) \ldots).$$

Anzitutto, essendo le p_r funzioni simmetriche delle x_i, esse non dovranno alterarsi allorchè in un modo comunque determinato si cambiano i segni dei radicali che entrano nelle x_i, giacchè un tale cambiamento produce soltanto una permutazione nell'ordine delle x_i stesse. Se p. es.

$$x = \sqrt{a + \sqrt{b}},$$

possiamo indicare i valori dell'espressione x con

$$\begin{aligned} x_1 &= +\sqrt{a + \sqrt{b}} \\ x_2 &= -\sqrt{a + \sqrt{b}} \\ x_3 &= +\sqrt{a - \sqrt{b}} \\ x_4 &= -\sqrt{a - \sqrt{b}}, \end{aligned}$$

ed allora si vede che cambiando il segno di $\sqrt{b}$, si permutano i valori di x_1, x_3 e di x_2, x_4; invece cambiando i segni di ambedue i radicali si permutano i valori di x_1, x_4 e di x_2, x_3; infine cambiando il segno del radicale esterno $\sqrt{a + \sqrt{b}}$, si permutano x_1, x_2 e x_3, x_4.

Ciò posto consideriamo p_r come un'espressione quadratica formata coi radicali che entrano nella x e supponiamo tale espressione posta sotto forma normale. Supposto che essa contenga termini d'ordine m, $\sqrt{X}$, $\sqrt{Y}$, $\sqrt{Z}$.... poniamo in evidenza il termine $\sqrt{X}$, scrivendo

$$p_r = P + Q\sqrt{X}.$$

Poichè p_r non cambia mutando il segno di $\sqrt{X}$, avremo allora

$$P + Q\sqrt{X} = P - Q\sqrt{X},$$

ossia

$$Q\sqrt{X} = 0,$$

e quindi

$$Q = 0.$$

Dunque p_r non dipende dal radicale $\sqrt{X}$. In modo analogo essa non dipende neppure da $\sqrt{Y}$, $\sqrt{X}$...., e perciò in essa figurano termini contenenti radicali, d'ordine $m-1$ al più.

Ma ripetendo il ragionamento precedente in relazione ai termini d'ordine $m-1$, si vede che p_r non può dipendere neppure da questi. Così proseguendo successivamente si prova che p_r non dipende da nessun radicale, ossia che p_r è un'espressione razionale (nel campo dato). Resta dunque stabilito che la $f(x)=0$ è un'equazione a coefficienti razionali $c \cdot d \cdot d$.

Abbiamo avvertito che fra i valori $x_1 x_2 \ldots$ di x possono trovarsene alcuni uguali fra loro; se p. es.

$$x = \sqrt{a+\sqrt{b}} + \sqrt{a-\sqrt{b}},$$

risultino uguali i valori di x ottenuti cambiando il segno di $\sqrt{b}$.

Poniamo di scegliere, fra i 2^n valori della x, tutti i valori *differenti;* sieno p. es. $x_1 x_2 \ldots . x_r$. Allora, l'equazione, di grado r,

$$\varphi(x) = (x-x_1)(x-x_2)\ldots(x-x_r) = 0,$$

ha anch'essa i coefficienti razionali; la cosa si dimostra come per la $f(x)=0$.

Paragonando le due equazioni

$$f(x)=0, \quad \varphi(x)=0,$$

si vede che la prima ammette tutte le radici della seconda, e però essa è riducibile, se $r<2^n$, avendosi

$$f(x) = \varphi(x)\psi(x),$$

ove $\psi(x)$ è un polinomio a coefficienti razionali.

§ 3. **Sul grado delle equazioni irriducibili risolubili per radicali quadratici.** — Dimostriamo anzitutto il teorema: *Se un'equazione algebrica a coefficienti razionali* (in un dato campo) *è soddisfatta da un valore dell'espressione quadratica* x, *essa è soddisfatta da tutti i valori della* x *ottenuti cambiando i segni dei radicali.*

Sia

$$F(x)=0,$$

l'equazione data.

Prendiamo x ridotta a contenere radicali indipendenti, e sotto forma normale, ponendo in evidenza un termine dell'ordine più alto m, $\sqrt{X}$:

$$x = A + B\sqrt{X}.$$

Sostituiamo questa espressione in F e riduciamo F a forma normale relativamente a $\sqrt{X}$, scrivendo

$$F(x) = L + M\sqrt{X};$$

L ed M dipendono razionalmente dagli altri termini di ordine m, $\sqrt{Y}$, $\sqrt{Z}$.... e dai termini d'ordine inferiore che figurano in x.

Ora si ha (per ipotesi)

$$F(x) = L + M\sqrt{X} = 0;$$

onde

$$L = M = 0,$$

oppure

$$\sqrt{X} = -\frac{L}{M};$$

ma quest'ultima relazione contraddice all'ipotesi che tutti i radicali contenenti in x sieno indipendenti; resta dunque provato che

$$L = M = 0,$$

e perciò

$$L - M\sqrt{X} = 0,$$

onde l'equazione

$$F(x) = 0,$$

è soddisfatta non soltanto da

$$x = A + B\sqrt{X},$$

ma anche da

$$x = A - B\sqrt{X}.$$

In modo analogo si prova che la $F(x) = 0$ è soddisfatta dai valori ottenuti mutando comunque nell'espressione di x, il segno dei termini d'ordine m, $\sqrt{Y}$, $\sqrt{Z}$....

Supponiamo, per semplicità di ragionamento, che in x entrino soltanto due termini dell'ordine m,

$$\sqrt{X} \quad \text{e} \quad \sqrt{Y},$$

avremo

$$F(x) = L + M\sqrt{X}$$

con

$$L = L_1 + L_2\sqrt{Y}$$
$$M = M_1 + M_2\sqrt{Y},$$

e, dall'essere $F(x) = 0$, concluderemo

$$L_1 = L_2 = M_1 = M_2 = 0.$$

Ora L_1, L_2, M_1, M_2 sono espressioni contenenti soltanto termini in cui figurano radicali, d'ordine $m - 1$ al più; col ragionamento precedente si prova che queste espressioni si annullano cambiando comunque in x il segno dei radicali dei termini d'ordine $m - 1$; se ne deduce che la $F(x) = 0$ è soddisfatta quando si cambino nell'espressione di x i segni dei radicali costituenti i termini dell'ordine $m - 1$.

È chiaro come il ragionamento si possa proseguire, pervenendo così alla conclusione che se l'equazione

$$F(x) = 0$$

è soddisfatta da un valore dell'espressione quadratica x, essa è pure soddisfatta da tutti quei valori che si ottengono dal dato cambiando segno in modo arbitrario ai radicali costituent i termini degli ordini

$$m, \quad m - 1, \quad m - 2, \ldots . 1.$$

Resta da far vedere che la $F(x) = 0$ è ancora soddisfatta se si cambiano i segni dei radicali che entrano sotto un altro radicale, p. es. i radicali costituenti i termini dell'espressione X che figura in $\sqrt{X}$. Ma ciò è stato già implicitamente dimostrato, perchè avendosi

$$F(x) = L + M\sqrt{X}$$

ove

$$L = M = 0,$$

sarà sempre

$$F(x) = 0,$$

comunque si cambi il segno dei radicali che figurano in X.

Dunque il teorema è completamente stabilito.

Esso conduce immediatamente al corollario:

Se un' equazione algebrica

$$F(x) = 0,$$

a coefficienti razionali, è soddisfatta da un valore di una espressione quadratica x, *e se si designa con*

$$\varphi(x) = 0,$$

l'equazione (a coefficienti razionali) del medesimo grado r, *a cui soddisfano tutti i valori differenti che la* x *può ricevere cambiando il segno dei radicali in essa contenuti, si ha*

$$F(x) = \varphi(x)\theta(x),$$

ove θ *è un polinomio a coefficienti razionali.*

Se la $F(x) = 0$ è un' equazione *irriducibile*, il polinomio θ si dovrà dunque ridurre ad un fattore costante.

Riprendiamo ora l'equazione $f(x) = 0$ innanzi considerata, cioè l'equazione, del grado 2^n, che ha per radici i 2^n valori dell'espressione quadratica x.

Abbiamo già avvertito che, se $r < 2^n$, si ha

$$f(x) = \varphi(x)\psi(x)$$

ove ψ è un polinomio a coefficienti razionali. Ora l'equazione $\psi(x) = 0$ ha per radici alcuni valori dell'espressione quadratica x, e quindi tutti i valori di essa; perciò si ha ancora

$$\psi(x) = \varphi(x)\psi_1(x) \quad \text{e} \quad f(x) = \varphi^2(x)\psi_1(x),$$

ove ψ_1 è un nuovo polinomio a coefficienti razionali, oppure una costante. Applichiamo a ψ_1 (supposto che non sia una costante) il ragionamento svolto relativamente a ψ, e così di seguito; in definitiva dovremo trovare un quoziente che si riduca ad una costante c, avendosi dunque

$$f(x) = c\varphi^s(x);$$

effettivamente la divisione non può procedere indefinitivamente avendo f un grado finito.

Ora avendosi, come si è detto,

$$f(x) = c\varphi^s(x),$$

ed essendo r il grado di φ, e 2^n il grado di f, sarà

$$rs = 2^n,$$

sicchè tanto r che s non contengono alcun fattore primo diverso da 2; in conclusione il grado dell'equazione

$$\varphi(x) = 0$$

sarà

$$r = 2^\nu.$$

Da ciò, ricordando i precedenti resultati, si deduce il teorema fondamentale:

Se un' equazione algebrica irriducibile è risolubile con soli radicali quadratici (in un dato campo di razionalità cui appartengono i suoi coefficienti), il suo grado è una potenza di 2.

Questa condizione necessaria non è però sufficiente; così p. es. un'equazione generale del 4° grado non è risolubile per radicali quadratici.

Le condizioni a cui deve soddisfare un' equazione di grado 2^ν, affinchè sia risolubile per radicali quadratici, ed i procedimenti da adoperarsi in generale per la risoluzione effettiva, sono stati ampiamente studiati da JULIUS PETERSEN in vari lavori. (Cfr. p. es. la citata « *Teoria delle equazioni algebriche* »).

II.

§ 4. **Riduzione del problema dei poligoni regolari alle equazioni binomie.** — Noi vogliamo applicare i risultati precedenti, relativi alle equazioni risolubili per radicali quadratici, al problema della costruzione dei poligoni regolari.

Dobbiamo anzitutto tradurre il problema sotto forma analitica. E perciò cominciamo a ricondurlo a tal forma, che sieno dati dei punti, e si cerchino punti aventi con essi relazioni prestabilite.

Bastano a tal fine le seguenti osservazioni semplicissime:

a) Tutti gli ngoni regolari sono simili fra loro, quindi il problema di costruire lo ngono regolare che ha un lato assegnato si riconduce subito al problema di costruire un qualsiasi ngono regolare. L'incognita è l'angolo del poligono, o, se si vuole, l'angolo al centro che proietta un lato; il lato compare nella questione come un parametro arbitrario.

b) Quando si sappia costruire un ngono regolare, si può anche costruire lo ngono regolare iscritto in un dato circolo e avente un dato vertice, cioè si può *dividere il circolo in* n *archi uguali* partendo da un punto di divisione assegnato, o viceversa.

Dunque il problema dei poligoni regolari è perfettamente equivalente a quello della divisione del circolo in n parti uguali, ove si può supporre che sieno dati il centro O del circolo ed un punto di divisione A. È lecito assumere la distanza dei due punti dati, cioè il raggio del circolo, come unità.

Sotto questa forma il problema, in cui i dati sono punti, è ricondotto alla ricerca di $n-1$ punti (di divisione) che, insieme ad A, costituiscono i vertici di un ngono regolare.

Ciascuno di questi punti determina con A (in uno qualunque dei due sensi) un arco che moltiplicato per n dà un multiplo dell'intero circolo, cioè un arco

$$\frac{2\pi r}{n}$$

(ove si può prendere $r < n$).

Riferiamoci a due assi coordinati ortogonali, prendendo O come origine ed OA come asse delle x. Il punto A avrà come coordinate 1, 0; i punti incogniti avranno certe coordinate

$$x_1 y_1, \quad x_2 y_2 \ldots x_{n-1} y_{n-1},$$

(soddisfacenti all'equazione

$$x^2 + y^2 = 1$$

del circolo), coordinate che appunto si tratta di determinare, partendo dalle sole quantità date 0, 1, le quali definiscono il campo di razionalità assoluto [1].

Immaginiamo rappresentati nel piano i valori della variabile complessa

$$z = x + iy$$

(rappresentazione di ARGAND-GAUSS). A ciascun valore z, corrispondono (come è noto) un *modulo*

$$\rho = \sqrt{x^2 + y^2}$$

e un *argomento*

$$\theta = \text{arc } tg \frac{y}{z},$$

coordinate polari del punto (xy) indice di z, sicchè si ha

$$z = \rho(\cos\theta + i \operatorname{sen}\theta).$$

Il modulo è la distanza assoluta del punto (xy) dall'origine *(raggio vettore)*: l'argomento è l'angolo *(anomalia)* che la congiungente il punto stesso coll'origine forma coll'asse x.

Ora la moltiplicazione di due numeri complessi

$$z = x + iy, \quad z' = x' + iy'$$

si può effettuare; algebricamente, secondo le ordinarie regole del calcolo, ponendo

$$Z = zz' = (xx' - yy') + i(xy' + x'y);$$

oppure geometricamente, determinando il punto che ha come coordinate polari

$$P = \rho\rho' = \sqrt{x^2 + y^2} \cdot \sqrt{x'^2 + y'^2}$$

$$\Theta = \theta + \theta' = \arg tg \frac{y}{z} + \text{arc } tg \frac{y'}{z'},$$

cioè facendo il prodotto dei moduli e la somma degli argomenti.

Applicando questa regola geometrica, formiamo le successive potenze dei numeri complessi

$$z_s = x_s + iy_s,$$

aventi come indici i nostri punti incogniti

$$(x_1 y_1), \ldots, (x_{n-1} y_{n-1}).$$

Il modulo

$$\sqrt{x_s^2 + y_s^2} = 1,$$

e l'argomento è

$$\frac{2\pi r}{n}$$

$$\left(\text{onde } z_s = \cos\frac{2\pi r}{n} + i \operatorname{sen}\frac{2\pi r}{n}\right).$$

quindi il modulo di z_s^n sarà sempre $= 1$, mentre il suo argomento sarà

$$\frac{2\pi rh}{n}.$$

In particolare per $h = n$, il punto z_s^n si troverà sulla parte positiva dell'asse delle x, e quindi coinciderà con

$$A \equiv (1,0);$$

per conseguenza

$$z_s^n = 1.$$

Viceversa si abbia un punto (xy), diverso dal punto A, tale che

$$z^n = (x + iy)^n = 1;$$

questo punto deve avere un modulo ρ tale che $\rho^n = 1$; e quindi un modulo $= 1$; inoltre esso deve avere un argomento θ che moltiplicato per n differisca da 0 per multipli di 2π, onde

$$\theta = \frac{2\pi r}{n};$$

dunque il detto punto è uno dei punti

$$(x_1 y_1) \ldots . (x_{n-1} y_{n-1})$$

che soddisfano al nostro problema.

In conclusione:

Il problema della costruzione di un ngono regolare, viene a dipendere dalla risoluzione dell' equazione binomia

$$z^n = 1,$$

e precisamente dalla ricerca delle radici di essa diverse da $z = 1$, *cioè dalla risoluzione dell' equazione*

$$\frac{z^n - 1}{z - 1} = z^{n-1} + z^{n-2} + \ldots . + 1 = 0.$$

Questa equazione si può scindere in due altre relative ad x e y; ma ciò non è necessario, nè utile. Se l'equazione indicata in z può essere risoluta per radicali quadratici (nel campo di razionalità [1] dato dai coefficienti), anche le coordi-

nate z, y dei punti incogniti verranno espresse per radicali quadratici, giacchè si ha

$$\sqrt{a+ib} = \sqrt{\frac{a}{2} + \sqrt{a+b^2}} + i\sqrt{\frac{a}{2} + \sqrt{a+b^2}},$$

e quindi lo ngono sarà costruibile colla riga e col compasso. Viceversa se lo ngono è costruibile, le x, y sono espressioni quadratiche e quindi anche le radici

$$z = x + iy$$

dell' equazione binomia, risulteranno pure esprimibili per radicali quadrati.

Il problema della costruzione elementare dei poligoni regolari è così ricondotto alla questione di risolvere (quando sia possibile), per radicali quadratici, l'equazione binomia

$$z^n = 1.$$

§ 5. **Irriducibilità dell'equazione $\frac{z^p-1}{z-1}=0$, quando p è un numero primo.** — Consideriamo l'equazione

$$z^p - 1 = 0$$

nell'ipotesi in cui p sia un numero primo. Togliendo il fattore lineare $z-1$, essa si riduce alla forma

$$F(z) = \frac{z^p-1}{z-1} = z^{p-1} + z^{p-2} + \ldots + z + 1 = 0.$$

Noi vogliamo dimostrare che questa equazione è irriducibile, nel campo assoluto di razionalità [1], cioè che $F(z)$ non può spezzarsi nel prodotto di due polinomi a coefficienti (numerici) razionali.

A tale scopo occorre premettere un lemma sopra la decomponibilità dei polinomi, lemma dovuto a GAUSS.

Si abbia un polinomio

$$f(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_n,$$

i cui coefficienti sieno numeri interi; diremo che questo poli-

nomio è *primitivo* allorchè i numeri $a_0 a_1 \ldots a_n$ non ammettono alcun divisore comune, diverso dall'unità.

Ora sieno

$$f(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_n,$$

e

$$\varphi(z) = b_0 z^m + b_1 z^{m-1} + \ldots + b_m$$

due polinomi a coefficienti interi, primitivi. Formiamo il prodotto

$$F(x) = f(x)\varphi(x) = c_0 z^{m+n} + c_1 z^{m+n-1} + \ldots c_{m+n},$$

dove

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0,$$

e in generale

$$c_h = a_0 b_h + a_1 b_{h-1} + \ldots + a_h b_0,$$

coll'avvertenza che

$$a_r = 0 \quad \text{per} \quad r > n,$$
$$b_s = 0 \quad \text{per} \quad s > m.$$

Mostriamo che il polinomio $F(x)$ è primitivo, cioè che non esiste alcun numero primo p (>1), il quale divida tutti i numeri $c_0, c_1 \ldots c_{m+n}$.

Dato un numero primo p (>1), questo non può dividere tutti i coefficienti a di f, nè i coefficienti b di φ; si troverà dunque un primo coefficiente a_r

$$(\text{con } r \leq n)$$

e così un primo coefficiente b_s

$$(\text{con } s \leq m)$$

i quali non saranno divisibili per p. Allora consideriamo il coefficiente

$$c_{r+s} = a_0 b_{r+s} + \ldots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \ldots + a_{r+s} b_0.$$

Tutti i termini della somma sono divisibili per p, tranne $a_r b_s$; dunque c_{r+s} non è divisibile per p.

L'osservazione precedente ci permette di dimostrare il

LEMMA DI GAUSS. — *Se un polinomio a coefficienti interi* F(z) *è riducibile, esso può decomporsi nel prodotto di due polinomi a coefficienti interi.*

Possiamo supporre, senza restrizione, che F sia un polinomio primitivo, altrimenti esso potrebbe porsi sotto la forma $\mu F'$ ove F' è primitivo e μ è un numero intero (divisore comune dei coefficienti di F), sicchè basterebbe evidentemente dimostrare il teorema per F'.

Ammettiamo dunque che $F(z)$ si decomponga nel prodotto di due polinomi $f(z)$ e $\varphi(z)$ a coefficienti razionali, e vogliamo provare che F riesce allora anche il prodotto di polinomi a coefficienti interi.

Riduciamo tutti i coefficienti di f ad avere il minimo comun denominatore a; i numeratori avranno allora un massimo comun divisore α primo con a. Operiamo nello stesso modo sui coefficienti di φ, riducendoli ad avere un minimo comun denominatore b; sia β il massimo comun divisore dei numeratori dei coefficienti così ridotti. Allora i polinomi $\frac{af}{\alpha}$ e $\frac{b\varphi}{\beta}$ avranno i coefficienti interi e saranno primitivi; il loro prodotto

$$\frac{ab}{\alpha\beta} f\varphi = \frac{ab}{\alpha\beta} F$$

sarà dunque un polinomio a coefficienti interi e primitivo.

Per la prima condizione, poichè i coefficienti di F non ammettono alcun divisore comune, ogni fattore primo contenuto in $\alpha\beta$ dovrà dividere ab, e perciò $\alpha\beta$ dividerà ab; per la seconda il quoziente $\frac{ab}{\alpha\beta} = c$ (che come si è detto è un numero intero) dovrà essere uguale ad 1, altrimenti tutti i coefficienti di cF sarebbero divisibili per $c > 1$.

In conclusione $F(z)$ è il prodotto di due polinomi a coefficienti interi e primitivi $\frac{a}{\alpha} f$ e $\frac{b}{\beta}\varphi$. *c. d. d.*

In base al lemma di GAUSS, si può facilmente dimostrare, usando del ragionamento di EISENSTEIN [1], che:

L'equazione $\frac{z^p - 1}{z - 1} = 0$, *dove* p *è un numero primo, è irriducibile.*

[1] « Crelle 's Journal - Bd. 39 » pag. 167. Due diverse dimostrazioni dello stesso teorema sono state date da KRONECHER « Crelle 's J. - Bd. 29 », e « Journal de Liouville 12, vol. 1 ». Cfr. BACHMANN, *l. c.*

Ponendo

$$z = x + 1$$

l'equazione predetta diventa

$$F(x) = x^{p-1} + px^{p-2} + \frac{p(p-1)}{2} x^{p-3} + \ldots + \\ + \binom{p}{r} x^{p-r-1} + \ldots + p = 0.$$

Basta evidentemente dimostrare l'irriducibilità della $F(x) = 0$, perchè dall'essere

$$\frac{z^p - 1}{z - 1} = \varphi_1(z) f_1(z)$$

ove φ_1, f_1 sono due polinomi, segue

$$F(x) = \varphi_1(x+1) f_1(x+1) = \varphi(x) f(x),$$

ove φ e f sono due polinomi in x.

Supponiamo che la $f(x) = 0$ sia riducibile, allora si avrà

$$f(x) = \varphi(x) f(x)$$

ove φ e f sono due polinomi in x, a coefficienti interi:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \\ \varphi(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m.$$

Eseguendo il prodotto φf si troverà un polinomio identicamente uguale ad F:

$$c_0 x^{n+m} + c_1 x^{n+m-1} + \ldots + c_{n+m},$$

il cui grado $n + m = p$.

Si avranno dunque le formule:

$$c_0 = a_0 b_0 = 1$$
$$c_1 = a_0 b_1 + a_1 b_0 = p$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = \frac{p(p-1)}{2}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$c_{n+m-1} = a_{n-1} b_m + a_n b_{m-1} = \frac{p(p-1)}{2}$$
$$c_{n+m} = a_n b_m = p,$$

e perciò tutti i coefficienti c, eccetto c_0, saranno divisibili per il numero primo p.

Ora l'ultima relazione scritta, appunto perchè p è un numero primo, porta che uno dei due numeri a_n, b_m sia uguale $a \pm 1$, e l'altro a $\pm p$; sia p. es.

$$a_n = 1, \quad b_m = p.$$

Sostituendo questi valori nella penultima relazione si trova

$$c_{n+m-1} = a_{n-1}p + b_{m-1},$$

e poichè p divide c_{n+m-1}, b_{m-1} è divisibile per p, ossia:

$$b_{m-1} = pb'_{m-1}.$$

Proseguendo analogamente a considerare l'espressione di c_{n+m-2}, si trova

$$c_{n+m-2} = a_{n-2}p + a_{n-1}b'_{m-1}p + b_{m-2},$$

e quindi b_{m-2} è divisibile per p, ossia:

$$b_{m-2} = pb'_{m-2}.$$

Successivamente dalle espressioni di $c_{n+m-3} \ldots c_n$ si ricava che sono divisibili per p tutti i coefficienti $b_{m-3} \ldots b_0$, ma la conclusione che si riferisce a b_0 si rivela subito assurda perchè l'uguaglianza

$$c_0 = a_0 b_0 = 1$$

dà

$$a_0 = \pm 1, \quad b_0 = \pm 1.$$

L'assurdo a cui si è condotti dall'ipotesi della decomponibilità di F, prova che l'equazione $F = 0$, e quindi la

$$\frac{z^p - 1}{z - 1} = 0$$

è irriducibile. *c. d. d.*

§ 6. **Impossibilità di costruire elementarmente i poligoni regolari di un numero primo p di lati, quando p non ha la forma $2^n + 1$.** — Ora ricordando il risultato fondamentale del § 3, concludiamo:

Se l'equazione $\frac{z^p-1}{z-1}=0$, *ove* p *è un numero primo è risolubile per radicali quadratici, deve essere* $p-1$ *una potenza del* 2 *e perciò:*

$$p=2^n+1.$$

E per conseguenza:

Non è possibile costruire colla riga e col compasso il poligono regolare avente un numero primo p *di lati, quando* p *non sia della forma* 2^n+1.

Così ad es. *non sono costruibili,* nel modo anzidetto, i poligoni regolari di 7, 11, 13, 19.... lati.

§ 7. **Costruibilità dei poligoni regolari di un numero primo p di lati, quando p ha la forma 2^n+1.** — A questo resultato negativo fa riscontro il seguente resultato positivo:

Il poligono regolare di p *lati ove* p *è un numero primo della forma* 2^n+1, *è costruibile colla riga e col compasso.*

Per dimostrare questo teorema, occorre far vedere che l'equazione (irriducibile)

$$\frac{z^p-1}{z-1}=z^{p-1}+z^{p-2}+\ldots.+z+1=0,$$

è risolubile con successive estrazioni di radici quadrate, quando p è un numero primo della forma 2^n+1.

Le radici della nostra equazione, cioè le radici p^{me} dell'unità, diverse da 1, sono

$$\varepsilon_1=\cos\frac{2\pi}{p}+i\,\mathrm{sen}\frac{2\pi}{p},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\varepsilon_r=\cos\frac{2\pi r}{p}+i\,\mathrm{sen}\frac{2\pi r}{p},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\varepsilon_{p-1}=\cos\frac{2\pi(p-1)}{p}+i\,\mathrm{sen}\frac{2\pi(p-1)}{p}.$$

Esse possono ottenersi tutte formando le successive potenze di una qualunque radice ε. Partendo p. es. dalla radice $\varepsilon=\varepsilon_1$, avremo infatti $\varepsilon_r=\varepsilon^r$.

Partendo dalla radice $\varepsilon = \varepsilon_2$, avremo

$$\varepsilon_2 = \varepsilon \quad \varepsilon_4 = \varepsilon^2 \quad \varepsilon_6 = \varepsilon^3 \ \ldots\ \varepsilon_{p-1} = \varepsilon^{\frac{p-1}{2}},$$

$$\varepsilon_1 = \varepsilon^{\frac{p-1}{2}+1} \qquad \varepsilon_3 = \varepsilon^{\frac{p-1}{2}+2} \qquad \varepsilon_7 = \varepsilon^{\frac{p-1}{2}+3}$$

$$\ldots\ \varepsilon_{p-2} = \varepsilon^{p-1}.$$

In modo analogo le potenze successive di una qualunque $\varepsilon = \varepsilon_r$, cogli esponenti $1, 2 \ldots p-1$, sono tutte diverse fra loro, e quindi riproducono (in altro ordine) le radici $\varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p-1}$. Invero non può aversi per $h < p$, $k < p$,

$$\varepsilon_r^{\,h} = \varepsilon_r^{\,k},$$

senza che si abbia

$$\varepsilon_r^{\,h-k} = 1$$

cioè

$$\cos \frac{2\pi r(h-k)}{p} + i \operatorname{sen} \frac{2\pi r(h-k)}{p} = 1,$$

onde

$$2\pi \frac{r(h-k)}{p} = 2\pi s$$

con s intero; e questa uguaglianza è assurda perchè, essendo p un numero primo ed $r < p$, p non può dividere $r(h-k)$ senza dividere $h-k$.

Si noti ancora che sussiste sempre l'uguaglianza

$$\varepsilon^{l+mp} = \varepsilon^l,$$

essendo

$$\varepsilon^{mp} = 1.$$

Volendo ora approfondire lo studio delle radici della nostra equazione, ci occorre prendere dalla teoria dei numeri il seguente teorema (1):

Dato un numero primo p, *esiste sempre fra i numeri* $1, 2 \ldots p-1$, *qualche numero* g, *tale che le potenze*

$$g, \quad g^2, \ldots\ g^{p-1},$$

(1) Cfr. p. es. U. SCARPIS: *Primi elementi della teoria dei numeri.* Hoepli 1897.

divise per p, *dieno per resti i numeri*

$$1, \quad 2 \ldots p-1$$

presi in altro ordine.

Un tal numero g si dice una *radice primitiva* del *modulo* p.

Se ad esempio $p=5$, prendendo a considerare il numero 2 si ha

$$2^1=2, \quad 2^2=4, \quad 2^3=8, \quad 2^4=16$$

e questi numeri divisi per 5 danno rispettivamente come resti

$$2, \quad 4, \quad 3, \quad 1,$$

onde 2 è una radice primitiva del modulo 5.

Nel caso di $p=7$, formando le potenze successive del 2 si ottengono i numeri

$$2^1=2, \quad 2^2=4, \quad 2^3=8, \quad 2^4=16, \quad 2^5=32, \quad 2^6=64$$

che divisi per 7 danno come resti

$$2, \quad 4, \quad 1, \quad 2, \quad 4, \quad 1,$$

e quindi 2 non è una radice primitiva del modulo 7. Invece le successive potenze del 3.

$$3^1=3, \quad 3^2=9, \quad 3^3=27, \quad 3^4=81, \quad 3^5=243, \quad 3^6=729$$

divise per 7 danno come resti

$$3, \quad 2, \quad 6, \quad 4, \quad 5, \quad 1,$$

onde il numero 3 è una radice primitiva del modulo 7.

Riferendoci al caso generale di un qualsivoglia numero p, supponiamo di aver determinato una radice primitiva g del modulo p, e consideriamo nuovamente una radice ε dell'equazione.

$$\frac{z^p-1}{z-1}=0.$$

Formando le successive potenze

$$\varepsilon^g \quad \varepsilon^{g^2} \quad \varepsilon^{g^3} \ldots \varepsilon^{g^{p-1}},$$

vediamo che queste riproducono in altro ordine le radici

$$\varepsilon \quad \varepsilon^2 \ldots \varepsilon^{p-1}.$$

Infatti, indicando con s_r il resto della divisione di g^r per p, avremo

$$(g^r = ph + s_r)$$

$$\varepsilon^{g^r} = \varepsilon^{s_r} \quad (\varepsilon^{p^h} = 1),$$

dove s_r prende (in altro ordine) tutti i valori $1, 2 \ldots p-1$, mentre r riceve successivamente i valori $1, 2 \ldots p-1$.

Ora dividiamo le radici

$$\varepsilon^g \quad \varepsilon^{g^2} \quad \ldots \quad \varepsilon^{g^{p-1}}$$

in due gruppi

$$\varepsilon^g \quad \varepsilon^{g^3} \quad \ldots \quad \varepsilon^{g^{p-2}}$$

$$\varepsilon^{g^2} \quad \varepsilon^{g^4} \quad \ldots \quad \varepsilon^{g^{p-1}},$$

e poniamo

$$\eta_1 = \varepsilon^g + \varepsilon^{g^3} + \ldots + \varepsilon^{g^{p-2}}$$

$$\eta_2 = \varepsilon^{g^2} + \varepsilon^{g^4} + \ldots + \varepsilon^{g^{p-1}}.$$

Dividiamo successivamente ciascuno dei gruppi formati innanzi, in altri due, ponendo

$$\left.\begin{aligned} \eta_{11} &= \varepsilon^g + \varepsilon^{g^5} + \ldots + \varepsilon^{g^{p-4}} \\ \eta_{12} &= \varepsilon^{g^3} + \varepsilon^{g^7} + \ldots + \varepsilon^{g^{p-2}} \end{aligned}\right\} \eta_{11} + \eta_{12} = \eta_1$$

$$\left.\begin{aligned} \eta_{21} &= \varepsilon^{g^2} + \varepsilon^{g^6} + \ldots + \varepsilon^{g^{p-3}} \\ \eta_{22} &= \varepsilon^{g^4} + \varepsilon^{g^8} + \ldots + \varepsilon^{g^{p-1}} \end{aligned}\right\} \eta_{21} + \eta_{12} = \eta_2.$$

In questo modo si può seguitare formando successivamente delle somme di

$$\frac{p-1}{4}, \quad \frac{p-1}{8} \ldots$$

termini, arrivando infine (*poichè* $p-1$ *è una potenza del* 2) a somme di un solo termine, cioè alle radici della nostra equazione. Le somme sopra indicate prendono il nome di *periodi di Gauss*. Noi mostreremo come questi periodi si possono calcolare con successive estrazioni di radici quadrate.

Osserviamo anzitutto che la somma

$$\eta_1 + \eta_2 = \eta = \varepsilon^g + \varepsilon^{g^2} + \ldots + \varepsilon^{g^{p-1}} = -1,$$

giacchè η è, a parte il segno, il coefficiente di z^{p-2} nella equazione

$$z^{p-1} + z^{p-2} + \ldots + 1 = 0$$

di cui le ε sono radici.

Consideriamo il prodotto $\eta_1 \eta_2$.

Eseguendo la moltiplicazione delle due somme costituenti η_1 e η_2, si ottiene una somma di termini del tipo

$$\varepsilon^{g^r} \varepsilon^{g^s} = \varepsilon^{g^r + g^s} = \varepsilon^h = \varepsilon^{g^t},$$

cioè una somma di termini ciascuno dei quali si trova in uno dei due gruppi costituenti η_1 o η_2.

Ora l'espressione

$$\eta_1 \eta_2 = \Sigma \varepsilon^t$$

non cambia quando in essa si sostituisca ε con ε^g, perchè una tale sostituzione produce soltanto (come è facile verificare) lo scambio di

$$\eta_1 \quad \text{con} \quad \eta_2 \quad \text{e di} \quad \eta_2 \quad \text{con} \quad \eta_1.$$

Questo fatto fondamentale porta di conseguenza che la somma $\Sigma \varepsilon^{g^t}$ contiene uno stesso numero ρ di volte ogni radice dell'equazione

$$\frac{z^p - 1}{z - 1} = 0,$$

e quindi si ha

$$\eta_1 \eta_2 = \Sigma \varepsilon^{g^t} = \rho \eta = -\rho.$$

Per vedere chiaramente come si arrivi a tale conseguenza, cominciamo a raggruppare nella somma i termini simili, scrivendo

$$\eta_1 \eta_2 = k \varepsilon^{g^r} + \lambda \varepsilon^{g^s} + \ldots,$$

e mostriamo che i coefficienti interi k, λ.... sono tutti uguali fra loro, al quale scopo basta mostrare che nessuno di essi può essere inferiore ad un altro arbitrariamente scelto.

Se ad es. nella anzidetta somma entra il termine $\rho \varepsilon^g$; sostituendo in esso ε con ε^g, si troverà il termine $\rho \varepsilon^{g^2}$ e da questo si dedurranno successivamente i termini $\rho \varepsilon^{g^3}$, $\rho \varepsilon^{g^4}$...., che dovranno tutti comparire nella somma stessa. Se nella somma compare il termine $\rho \varepsilon^{g^2}$, sostituendo in esso ε con ε^g

ed operando successivamente la medesima sostituzione nei termini via via ottenuti, troveremo i termini

$$\rho\varepsilon g^3, \quad \rho\varepsilon g^4 \ldots \rho\varepsilon g^{p-1}, \quad \left(\rho\varepsilon g^p = \rho\varepsilon g\right)$$

i quali tutti dovranno comparire similmente nella somma stessa.

E così in generale dall'esistenza del termine $\rho\varepsilon g^t$ si deduce che la somma deve contenere tutti i termini

$$\rho\varepsilon g^{t+1} \; \rho\varepsilon g^{t+2} \ldots \rho\varepsilon g^{t+p-1}$$

i quali riproducono in altro ordine

$$\rho\varepsilon g \; \rho\varepsilon g^2 \ldots \rho\varepsilon g^{p-1}.$$

Dunque abbiamo che $\eta_1 + \eta_2$ ed $\eta_1\eta_2$ sono numeri interi, e perciò η_1, η_2 soddisfano ad un'equazione di 2° grado:

$$x^2 + x - \rho = 0$$

a coefficienti interi.

Tale equazione si risolve coll'estrazione del radicale $\sqrt{1+4\rho}$, per mezzo del quale η_1 e η_2 vengono espressi.

Procediamo ora al calcolo dei periodi di $\frac{p-1}{4}$ termini

$$\eta_{11}, \quad \eta_{12}, \quad \eta_{21}, \quad \eta_{22}.$$

Si ha anzitutto

$$\eta_{11} + \eta_{12} = \eta_1, \quad \eta_{21} + \eta_{22} = \eta_2.$$

Ora formiamo i prodotti

$$\eta_{11}\eta_{12}, \quad \eta_{21}\eta_{22}.$$

Considerando ad es. il primo di questi prodotti, vediamo che esso può ridursi ad una somma di termini del tipo εg^t, e precisamente ad una somma che non cambia quando si sostituisca in ogni termine ε con εg^2; infatti per tale sostituzione i periodi η_{11} e η_{12} vengono soltanto scambiati l'uno coll'altro. Da ciò si desume (come innanzi) che se l'espressione di $\eta_{11}\eta_{12}$ contiene un certo numero ρ_1 di volte un termine di η_1, essa

contiene altrettante volte gli altri termini della stessa somma (se ad es. $\eta_{11}\eta_{12}$ contiene il termine $\rho_1\varepsilon^g$, contiene pure $\rho_1\varepsilon^{g^3}$, $\rho_1\varepsilon^{g^5}$....); analogamente se l'espressione suddetta contiene ρ_2 volte un termine di η_2, essa contiene ρ_2 volte tutti gli altri termini, sicchè

$$\eta_{11}\eta_{12} = \rho_1\eta_1 + \rho_2\eta_2$$

ove ρ_1 e ρ_2 sono numeri interi.

Quindi η_{11}, η_{12} sono radici dell'equazione di 2° grado

$$x^2 - \eta_1 x + (\rho_1\eta_1 + \rho_2\eta_2) = 0.$$

Così $\eta_{11}\eta_{12}$ si possono calcolare coll'estrazione d'una radice quadrata, partendo da η_1, η_2. Analogamente si ottengono η_{21}, η_{22}.

È chiaro ormai come si possa procedere successivamente al calcolo dei periodi di $\frac{p-1}{8}$ termini.

Considerando ad es. η_{111}, η_{112}, la loro somma è

$$\eta_{111} + \eta_{112} = \eta_{11},$$

ed il loro prodotto si esprime con una combinazione lineare a coefficienti interi di η_{11}, η_{12}, η_{21}, η_{22}; così $\eta_{111}\eta_{112}$ si ottengono coll'estrazione d'un nuovo radicale quadratico che porta sopra i periodi ottenuti innanzi.

Proseguendo nello stesso modo si possono costruire i periodi di

$$\frac{p-1}{16}, \quad \frac{p-1}{32} \ldots$$

termini, e finalmente i periodi di un termine

$$\left(\frac{p-1}{2^n} = 1\right),$$

cioè le radici ε dell'equazione proposta.

Possiamo dunque concludere: *Quando* p *è un numero primo della forma* $2^n + 1$, *l'equazione*

$$\frac{z^p - 1}{z - 1} = 0$$

si può risolvere con successive estrazioni di radici quadrate, quindi il poligono regolare di p *lati è costruibile colla riga e col compasso.*

Osservazione. Nel ragionamento precedente non abbiamo tenuto conto dell'ambiguità che si presenta nella scelta dei segni da attribuirsi ai radicali quadratici successivamente introdotti. E di tale ambiguità non occorre invero preoccuparsi, quando si ha in vista di mostrare soltanto come i periodi η possono esprimersi mediante radicali quadratici, e quindi la stessa equazione data $\frac{z^p - 1}{z - 1} = 0$ sia risolubile mediante i radicali suddetti. Procedendo alla risoluzione effettiva, ove si lasci sussistere l'indeterminatezza dei segni dei nominati radicali, si troveranno tutte le radici ε dell'equazione proposta. Ma se venisse assegnata *a priori* una particolare radice ε per la costruzione dei periodi η_i, volendo giungere al calcolo di essa, si dovrebbe via via determinare i segni suindicati in modo conveniente. Le particolari regole di determinazione che qui occorrono, si troveranno spiegate, pel caso $p = 17$, nell'art. 6°, ove hanno un'interesse per la costruzione effettiva dell'ettadecagono.

§ 8. **Sui numeri primi della forma** $2^n + 1$. — I resultati ottenuti diventano più espressivi in forza della seguente osservazione:

Ogni numero primo della forma $2^n + 1$ *è un numero della forma* $2^{2^\nu} + 1$, vale a dire se $2^n + 1$ è un numero primo, n deve essere, alla sua volta, una potenza del 2.

Per giustificare questa proposizione, basta notare che se n ammette qualche divisore dispari

$$2k + 1 \quad [n = h(2k + 1)],$$

il numero

$$2^n + 1 = 2^{h(2k+1)} + 1$$

non può essere primo.

Ora si riconosce subito che il numero $2^{h(2k+1)}$ non può esser primo, essendo divisibile per $2^h + 1$. Infatti il binomio

$$x^{2h+1} + 1$$

si annulla per $x = -1$ e perciò è divisibile per $x+1$:

$$x^{2h+1}+1 = (x+1)[x^{2h} - x^{2h-1} + \ldots. + (-1)^r x^{2h-2} + \ldots. + 1];$$

facendo

$$x = 2^h$$

si ha appunto che $2^{h(2k+1)}+1$ è divisibile per 2^h+1.

Ora i resultati dei numeri precedenti si possono enunciare dicendo:

I poligoni regolari di un numero primo p *di lati, costruibili colla riga e col compasso, sono quelli per cui* p *è della forma*

$$p = 2^{2^\nu}+1.$$

Per vedere la portata di questo enunciato, diamo a ν i valori

$$\nu = 0,\quad 1,\quad 2,\quad 3,\quad 4;$$

otteniamo dalla formula

$$p = 2^{2^\nu}+1$$

i numeri primi

$$3,\quad 5,\quad 17,\quad 257,\quad 65537.$$

I valori 1, 3 e 5 di p corrispondono ai casi notissimi del triangolo equilatero e del pentagono regolare; mentre i valori successivi danno luogo a tre nuovi poligoni regolari costruibili, fra i quali è particolarmente notevole il caso $p = 17$. La risoluzione dell'equazione binomia $z^{17} = 1$ fu data dal GAUSS, ed alle costruzioni geometriche dell'ettadecagono si volsero successivi lavori (LEGENDRE, GRUNERT, STAUDT, SERRET, SCHRÖTER, GÉRARD) dei quali è dato un resoconto nell'art. 6°.

Il caso $p = 257$ fu studiato da RICHELOT [1], i resultati di lui furono interpretati geometricamente dal sig. AFFOLTER e dal sig. PASCAL [2].

Il caso $p = 65537$ è stato oggetto di un accuratissimo studio del sig. HERMES [3].

(1) *Crelle's Journal*, Bd. 9.
(2) *Rendic. della R. Accademia di Napoli*, 1887.
(3) Cfr. GÖTTINGER, *Nachrichten*, 1894.

Ora che cosa accade per $\nu > 4$? Si otterranno ancora dei numeri primi

$$p = 2^{2^\nu} + 1,$$

e quindi dei nuovi poligoni regolari costruibili?

I casi finora studiati si riferiscono ai numeri corrispondenti a

$$\nu = 5, \quad 6, \quad 7,$$

cioè ai numeri

$$2^{2^5} + 1, \quad 2^{2^6} + 1, \quad 2^{2^7} + 1,$$

i quali sono composti.

Pertanto resta dubbio se la serie dei numeri

$$2^{2^\nu} + 1$$

comprenda altri numeri primi, all'infuori di quelli corrispondenti ai valori

$$\nu = 0, \quad 1, \quad 2, \quad 3, \quad 4.$$

§ 9. **Applicazione del metodo di Gauss al caso del pentagono regolare.** — Daremo infine, come esempio, l'applicazione del metodo esposto alla risoluzione dell'equazione

$$z^5 = 1,$$

da cui dipende la costruzione del pentagono regolare.

Le radici della equazione predetta sono

$$1, \quad \varepsilon, \quad \varepsilon^2, \quad \varepsilon^3, \quad \varepsilon^4,$$

ove

$$\varepsilon = \cos\frac{2\pi}{5} + i \operatorname{sen}\frac{2\pi}{5}.$$

Scegliamo una radice primitiva del modulo 5, e sia $g = 2$; allora le ε verranno ordinate nel modo seguente:

$$\varepsilon^2, \quad \varepsilon^4, \quad \varepsilon^8 = \varepsilon^3, \quad \varepsilon^{16} = \varepsilon.$$

I periodi binari sono dati da

$$\eta_1 = \varepsilon^2 + \varepsilon^3, \quad \eta_2 = \varepsilon^4 + \varepsilon;$$

e si ha

$$\eta_1 + \eta_2 = \eta = -1$$
$$\eta_1\eta_2 = (\varepsilon^2 + \varepsilon^3)(\varepsilon^4 + \varepsilon) = \varepsilon^6 + \varepsilon^3 + \varepsilon^7 + \varepsilon^4 =$$
$$= \varepsilon + \varepsilon^3 + \varepsilon^2 + \varepsilon^4 = \eta = -1,$$

onde η_1 e η_2 sono le radici dell'equazione

$$x^2 + x - 1 = 0,$$

cioè

$$\eta_1 = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$$
$$\eta_2 = -\frac{1}{2} \mp \frac{1}{2}\sqrt{5}.$$

Consideriamo i periodi di un termine

$$\eta_{21} = \varepsilon^4 \quad \eta_{22} = \varepsilon,$$

dove

$$\eta_{21} + \eta_{22} = \eta_2$$
$$\eta_{21}\eta_{22} = \varepsilon^5 = 1,$$

costruiremo l'equazione di 2° grado

$$x^2 - \eta_2 x + 1 = 0,$$

e risolvendola otterremo

$$\varepsilon = \frac{1}{4}\left\{-1 \mp \sqrt{5} \pm \sqrt{-10 \pm 2\sqrt{5}}\right\}$$

ossia

$$\varepsilon = \frac{1}{4}\left\{-1 \mp \sqrt{5} \pm i\sqrt{10 \mp 2\sqrt{5}}\right\}.$$

Le 4 radici ε dell'equazione binomia sono date da questa formula ove si attribuiscano ai radicali i segni + e —. Si può riconoscere geometricamente (in modo molto facile) che la radice

$$\varepsilon = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\,\frac{2\pi}{5}$$

viene data assumendo tutti i radicali positivamente, cioè ponendo

$$\varepsilon = \frac{1}{4}\left\{-1 + \sqrt{5} + i\sqrt{10 + 2\sqrt{5}}\right\}.$$

La formula

$$\eta_2 = 2\cos\frac{2\pi}{5} = -\left(\frac{1}{2} + \sqrt{5}\right)$$

dà una semplicissima costruzione del pentagono regolare.

§ 10. **Poligoni regolari con un numero di lati composto.** — Diciamo ora qualche cosa intorno alla costruibilità dei poligoni regolari di n lati, dove n è un numero composto. Anzitutto osserviamo che se n si decompone nel prodotto di due numeri interi p, q:

$$n = pq,$$

dato lo $n$gono regolare si costruiranno subito il $p$gono e il $q$gono. Infatti dato l'arco di cerchio $\frac{2\pi}{n}$ (la cui corda è il lato dello $n$gono), o, se si vuole, dato il relativo angolo al centro, basterà moltiplicarlo per q per ottenere l'arco o angolo

$$\frac{2\pi q}{n} = \frac{2\pi}{p},$$

da cui dipende la costruzione del $p$gono.

Pongasi ora che n sia scomposto nei suoi fattori primi $p_1, p_2, \ldots p_r$:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

Affinchè la costruzione dello $n$gono sia possibile, dovrà esser possibile la costruzione dei poligoni regolari di $p_1^{\alpha_1}$, $p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ lati.

La costruzione del poligono regolare di p^α lati, $(\alpha > 1)$, dipende dalla risoluzione dell'equazione binomia

$$z^{p^\alpha} = 1,$$

la quale (come è chiaro anche geometricamente) ammette tutte le radici dell'equazione

$$z^{p^{\alpha-1}} = 1.$$

L'equazione

$$\frac{z^{p^\alpha} - 1}{z^{p^{\alpha-1}} - 1} = 0$$

è irriducibile.

Questo teorema si dimostra collo stesso ragionamento di EISENSTEIN che ha servito pel caso $\alpha = 1$ (§ 5).

Da esso discende la conseguenza che l'equazione anzidetta sarà risolubile per radicali quadratici, solo quando il suo grado $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ sia una potenza del 2. Ma il numero $p^{\alpha-1}$ ove $\alpha > 1$, non può essere una potenza del 2 se non è $p = 2$.

Di qui si deduce che non vi è alcun poligono regolare costruibile di p^α lati, ove

$$\alpha > 1, \quad p > 2.$$

Dunque se lo ngono regolare è costruibile, il numero

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

deve contenere, all'infuori di una certa potenza del 2, tutti fattori primi differenti (elevati alla potenza 1), e questi fattori p debbono essere ciascuno della forma $2^{2^\nu}+1$, giacchè il poligono regolare di p lati deve risultare costruibile (§ 8); insomma il numero n deve essere della forma

$$n = 2^\nu \left(2^{2^{\nu_1}}+1\right)\left(2^{2^{\nu_2}}+1\right)\ldots\left(2^{2^{\nu_s}}+1\right),$$

ove $\nu_1, \nu_2 \ldots \nu_s$ sono tutti differenti fra loro, e

$$p_1 = 2^{2^{\nu_1}}+1, \quad p_2 = 2^{2^{\nu_2}}+1 \ldots$$

sono numeri primi.

Dimostriamo infine che quando n è un numero della forma indicata, la costruzione dello ngono regolare è effettuabile.

A tal fine basta far vedere come « dati i poligoni regolari di r, s lati ove r, s sono numeri primi fra loro, si possa costruire il poligono regolare di $n = rs$ lati ».

Supponendo dati i poligoni regolari di r, s lati, sono dati gli angoli al centro corrispondenti

$$a = \frac{2\pi}{r}, \quad b = \frac{2\pi}{s}.$$

Ora, essendo r e s primi fra loro, si può risolvere l'equazione d'analisi indeterminata

$$sx - ry = 1,$$

determinando due numeri interi x, y che vi soddisfino; allora si avrà

$$ax - by = 2\pi\left(\frac{x}{r} - \frac{y}{s}\right) = \frac{2\pi}{rs} = \frac{2\pi}{n}$$

e perciò si otterrà la costruzione dell'angolo al centro dello ngono (e quindi la costruzione dello ngono stesso) facendo la differenza tra gli angoli ax e by.

Come esempio consideriamo il caso del pentadecagono regolare ($n = 15$), la cui costruzione si può dedurre da quelle del triangolo equilatero e del pentagono regolare. Risolviamo l'equazione d'analisi indeterminata

$$3x - 5y = 1,$$

ponendo

$$x = 2, \quad y = 1.$$

L'angolo al centro del pentadecagono si costruisce quindi facendo la differenza fra il doppio dell'angolo al centro del pentagono e l'angolo al centro del triangolo equilatero:

$$\frac{2\pi}{15} = 2 \cdot \frac{2\pi}{5} - \frac{2\pi}{3}.$$

Questa costruzione non differisce sostanzialmente da quella di EUCLIDE ove si biseca l'angolo

$$\frac{2\pi}{3} - \frac{2\pi}{5} = \frac{4\pi}{15}.$$

Riassumendo infine i resultati ottenuti, possiamo enunciare il teorema:

Gli ngoni regolari costruibili colla riga e col compasso sono, tutti e soli, quelli per i quali il numero n *decomposto in fattori primi, è della forma*

$$n = 2^{\nu} \cdot \left(2^{2^{\nu_1}} + 1\right) \cdot \left(2^{2^{\nu_2}} + 1\right) \ldots \left(2^{2^{\nu_s}} + 1\right),$$

ove $\nu_1, \nu_2 \ldots \nu_s$ *sono differenti fra loro.*

§ 11. **Osservazioni sulla determinazione dei poligoni regolari che non sono costruibili elementarmente.** — Termineremo questo articolo con alcune osservazioni relative alla determinazione dei poligoni regolari che non sono costruibili colla riga e col compasso. E riferendoci al più semplice caso di un poligono regolare di p lati, ove p è un numero primo, spiegheremo sopra un esempio che cosa c'insegni a tale proposito il metodo di GAUSS per la risoluzione dell'equazione binomia:

$$z^p = 1.$$

Prendiamo dunque $p = 7$, e consideriamo le radici dell'equazione $z^7 = 1$ (tolta la $z = 1$):

$$\varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \varepsilon^4,\ \varepsilon^5,\ \varepsilon^6,$$

ove

$$\varepsilon = \cos\frac{2\pi r}{7} + i\,\mathrm{sen}\frac{2\pi r}{7}.$$

Scegliamo una radice primitiva del modulo 7, e sia $g = 3$; essa ci permette di ordinare le ε nel modo seguente:

$$\varepsilon^3,\ \varepsilon^{3^2} = \varepsilon^2,\ \varepsilon^{3^3} = \varepsilon^6,\ \varepsilon^{3^4} = \varepsilon^4,\ \varepsilon^{3^5} = \varepsilon^5,\ \varepsilon^{3^6} = \varepsilon.$$

Formiamo i periodi di 3 termini

$$\eta_1 = \varepsilon^3 + \varepsilon^{3^3} + \varepsilon^{3^5} = \varepsilon^3 + \varepsilon^6 + \varepsilon^5$$

$$\eta_2 = \varepsilon^{3^2} + \varepsilon^{3^4} + \varepsilon^{3^6} = \varepsilon^3 + \varepsilon^4 + \varepsilon;$$

abbiamo

$$\eta_1 + \eta_2 = \eta = -1 \quad (\eta = \Sigma\varepsilon)$$

$$\eta_1\eta_2 = (\varepsilon^3 + \varepsilon^6 + \varepsilon^5)(\varepsilon^2 + \varepsilon^4 + \varepsilon) = \varepsilon^5 + \varepsilon^7 + \varepsilon^4 + \varepsilon^8 + \varepsilon^{10} + \varepsilon^7 + \varepsilon^7 + \varepsilon^9 + \varepsilon^6 = \eta + 3 = 2,$$

e quindi η_1, η_2 soddisfano all'equazione di 2° grado

$$x^2 + x + 2 = 0.$$

Una volta calcolati η_1, η_2, la determinazione delle radici ε

viene a dipendere da un'equazione di 3° grado; infatti si ha per es.

$$\varepsilon^2 + \varepsilon^4 + \varepsilon = \eta_2$$
$$\varepsilon^2 \cdot \varepsilon^4 + \varepsilon^2 \cdot \varepsilon + \varepsilon^4 \cdot \varepsilon = \eta_1$$
$$\varepsilon^2 \cdot \varepsilon^4 \cdot \varepsilon = 1,$$

e quindi ε^2, ε^4, ε sono radici dell'equazione

$$x^3 - \eta_2 x^2 + \eta_1 x - 1 = 0.$$

Dalla effettuata riduzione dipende la *possibilità di ricondurre la costruzione dell' ettagono regolare alla trisezione d'un angolo* (cfr. art. 7°).

Il problema generale dell'equazione binomia $z^p = 1$, ove p è un numero primo qualunque, ammette sempre una riduzione (come per $p = 7$), potendosi ricondurre alla risoluzione di una serie di equazioni di grado inferiore: se $p - 1$, decomposto in fattori primi, è della forma

$$p - 1 = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \ldots,$$

si dovranno risolvere precisamente

α_1 equazioni successive di 2° grado,
α_2 equazioni del 3°,
α_3 equazioni del 5° ecc.

Una tale riduzione è portata dal metodo di GAUSS che conduce a formare successivamente periodi di

$$\frac{p-1}{2}, \quad \frac{p-1}{4}, \ldots \quad \frac{p-1}{2^{\alpha_1}}$$

termini, quindi periodi di

$$\frac{p-1}{2^{\alpha_1} \cdot 3} \ldots \frac{p-1}{2^{\alpha_1} 3^{\alpha_2}}$$

termini, periodi di

$$\frac{p-1}{2^{\alpha_1} 3^{\alpha_2} \cdot 5} \ldots \frac{p-1}{2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3}}$$

termini ecc. (1).

(1) Cfr. BACHMANN *l. c.*, BIANCHI *l. c.*, ove sono pure date le formule per la risoluzione effettiva.

Dal punto di vista geometrico c'interessano i primi casi, in cui $p-1$ ha soltanto fattori primi uguali a 2 e a 3, potendosi allora assegnare delle semplici costruzioni del $p$gono, ricorrendo ad un *trisettore degli angoli* o ad una *parabola fissa*, mezzi che in unione alla riga ed al compasso permettono di risolvere tutti i problemi di 3° grado (cfr. art. 7°).

Qui ci limiteremo a citare i seguenti lavori che trattano i casi più semplici: Per $p=7, 13, 97$ si può vedere: PASCAL, *Giornale di Matematiche di Battaglini*, vol. XXV; per $p=19, 37$: I. AMALDI, *ibidem*, vol. XXX.